UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
EASTERN DIVISION

MICHAEL ROSEN, *on behalf of himself and all others similarly situated*, Plaintiffs, v. GREYLOCK MCKINNON ASSOCIATES, INC., Defendant.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL

Plaintiff Michael Rosen ("Plaintiff") brings this action individually and on behalf of all others similarly situated against Defendant Greylock McKinnon Associates, Inc. ("Defendant" or "Greylock") and alleges the following:

NATURE OF THE ACTION

1. This Complaint is brought by Plaintiff and those similarly situated against Greylock because of its failure to adequately protect the sensitive personal and confidential information of Plaintiff and similarly situated individuals ("Class Members"), including, but not limited to Plaintiff's and the Class Members' home addresses, dates of birth, and Social Security numbers, financial account numbers, medical information, and health insurance claim numbers (collectively, "PII").

2. This information was compromised in a massive security breach (the "Breach") of Greylock's network systems that was publicly disclosed on April 8, 2024. According to a letter sent by Greylock to Plaintiff and other affected individuals, Greylock learned of the Breach on

May 30, 2023, approximately eleven (11) months prior to sending notice to those affected. A true and correct copy of the letter received by Plaintiff is attached hereto as Exhibit A.

3. As a result, Plaintiff and other affected Class Members have been deprived of the opportunity to quickly take the necessary measures to protect their PII and minimize potential harm.

PARTIES

4. Plaintiff Michael Rosen resides in Lakewood, Houston, Texas.

5. Greylock is a consulting firm with headquarters located at 75 Park Plaza, Fourth Floor, Boston, MA 022116.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d), as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interests and costs, and is a class action in which some members of the Class are citizens of states different than Greylock. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

7. This Court has personal jurisdiction over Greylock because Greylock has sufficient minimum contacts with the state of Massachusetts by way of the business it conducts in Massachusetts. Greylock avails itself to the laws of Massachusetts through the business it conducts, accordingly, this Court has general personal jurisdiction of Massachusetts.

8. Venue is proper pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Defendant Greylock Experiences a Cyber Attack.

9. Greylock "provides expert economic analysis and litigation support to a diverse group of domestic and international clients in the legal profession, the business community, and government agencies."[1] Greylock received Plaintiff and Class Members' PII in its provisions of services to its clients.

10. Plaintiffs and the Class Members trusted Greylock to safeguard their PII. Greylock owes Plaintiff and the Class Members a duty to use reasonable care to protect their PII from unauthorized access.

11. On May 30, 2023, Greylock learned that it had experienced a "sophisticated cyberattack" involving Plaintiff's personal information. *See* Exhibit A.

12. Upon information and belief, the Breach affected upwards of 341,000 individuals.

13. On April 8, 2024, Greylock distributed a letter to the affected individuals warning them that their highly sensitive PII had been compromised. Greylock's announcement came nearly eleven (11) months ***after*** the Breach occurred.

14. As a result of the delay, Greylock prevented Plaintiff and the Class Members from taking important protective measures to ensure their PII was safe. Greylock has provided no explanation for the delay in notifying Plaintiff and the Class Members.

15. The PII subject to the Breach contains sensitive information. By way of example but not limitation, Greylock identified the following as the information stolen in the Breach: names, dates of birth, Medicare Health Insurance Claim Numbers, Social Security Numbers, and "some medical information and/or health insurance information." *See* Exhibit A.

[1] https://www.gma-us.com/ (last accessed May 29, 2024).

16. Indeed, this PII is incredibly valuable because it is essential to conduct everyday business – from applying for employment or government benefits, to securing financing for major purchases such as a home or a vehicle. In the wrong hands, it can allow a person to commit harmful and serious crimes such as financial fraud and identity theft.

B. Greylock Had Inadequate Measures in Place to Prevent the Breach.

17. Greylock is, and at all relevant times has been, aware the PII it collects and maintains on behalf of its clients is highly sensitive and could be used for nefarious purposes by unauthorized third parties.

18. Despite that knowledge, Greylock's safeguards were inadequate and failed on or around May 30, 2023. Despite acknowledging the Breach as a "sophisticated cyberattack," Greylock then characterized the attack as an "incident," and seemingly attempted to downplay the seriousness of the Breach in its letter sent to Plaintiff and Class Members eleven (11) months after the Breach occurred.

19. Greylock knew or should have known that its systems were vulnerable to an attack such as this, and should have (but did not) take extensive measures to safeguard its clients' PII.

C. Greylock Falls Short of FTC Compliance with Regard to Confidential Consumer Data Security.

20. Greylock, through its failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, has violated Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

21. First published in 2007, but updated in 2016, The Federal Trade Commission's ("FTC") document "Protecting Personal Information: A Guide for Business" highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks. These guidelines advise business to take the

following steps to establish reasonable data security practices" protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies and procedures for installing vendor-approved patches to correct security problems. The guidelines also recommend that business consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[2]

22. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

23. The FTC has issued orders against businesses that violated the FTC Act by failing to employ reasonable measures to secure consumer PII. Not only do these orders serve as enforcement mechanisms, but they also provide further guidance to businesses with regard to their data security obligations.

24. Greylock, well-aware of their obligations to implement fair and reasonable safeguards to protect clients' PII under the FTC Act, has fallen short of fulfilling these responsibilities and exposed its clients to high-risk data breaches.

D. Greylock Fails to Comply with the Health Insurance Portability and Accountability Act ("HIPAA").

25. Greylock is a covered entity under HIPAA. 45 C.F.R. § 160.102. Accordingly, it is

[2] FEDERAL TRADE COMMISSION, Protecting Personal Information: A Guide for Business (Nov. 2011), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 29, 2024).

required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R Part 160 and 164, Subparts A and C.

26. The Privacy Rule and Security Rule establish national standards for protecting health information and for protecting health information that is kept or transferred in electronic form.

27. HIPAA requires covered entities, like Greylock, to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronically protected health information." 45 C.F.R. § 164.302.

28. HIPAA defines "Electronic protected Health Information" as "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

29. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronically protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

30. Further, HIPAA requires Greylock to "review and modify the security measures

implemented . . . as needed to continue provision of reasonable and appropriate protection of electronically protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that been granted access rights." 45 C.F.R. § 164.312(a)(1).

31. Finally, the HIPAA Breach Notification Rule requires Greylock to provide notice of a data breach to each affected individual "without unreasonable delay in no case later than 60 days following the discovery of the breach." 45 C.F.R. §§ 160.400-414.

32. Greylock did not provide notice of the Breach for approximately eleven (11) months in further violation of HIPAA.

33. Greylock through its failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer health data, has violated HIPAA.

E. Greylock's Response to the Data Breach is Insufficient.

34. The untimely and inadequate notification of the Breach has damaged Plaintiff and Class Members. Greylock should have timely disclosed to Plaintiff and Class Members that their PII was compromised. A timely disclosure would have allowed Plaintiff and Class Members to take appropriate measures to monitor and protect their PII.

35. In addition, Greylock's offer of two years of free credit monitoring is inadequate. Data thieves will be aware of the temporal scope of the protection offered to Plaintiff and the Class Members and can simply wait out the time as is the practice of such cyber criminals.

36. Greylock's proposed remedy does nothing to protect the approximately 341,000 individuals who had their PII exposed to criminals, and does not ensure protection from fraud going forward.

37. Indeed, Plaintiff's and Class Members' stolen PII may also be sold on the "dark web" at some undetermined point in the future.

38. Credit monitoring and identity theft protection does not prevent actual fraud. Because cyber criminals can use the PII from the Breach to drain bank accounts, steal tax refunds, apply for loans, or open utility accounts, Plaintiff and Class Members still must employ heightened scrutiny to ensure that their PII is not being misappropriated. These are the harms that Plaintiff and Class Members can suffer far into the future, long after Greylock stops providing its clients credit monitoring or identity theft protection.

39. Furthermore, Greylock's failure to adequately protect its customers' PII had resulted in customers having to undertake various tasks (e.g., obtaining credit monitoring, checking, credit reports, motoring accounts, etc.) that require time and effort that they would otherwise not have expended on these efforts. At the same time, Greylock has withheld important details about the Breach as it conducts its investigation and is putting the burden on the individuals affected by the Breach to discover possible fraudulent transactions.

40. All of this translates into, according to the Department of Justice, victims of "misuse of. . . personal information to open a new account or conduct other fraud," the exact type of fraud to which Greylock has exposed its clients, "spen[ding] a mean of 7 hours resolving the problems.[3]

F. Plaintiff's Experience.

41. Plaintiff is a resident of Houston, Texas.

42. Plaintiff's PII was obtained by Greylock's client, the Department of Justice ("DOJ"), as part of a civil litigation matter. *See* Exhibit A.

[3] https://bjs.ojp.gov/document/vit21.pdf

43. In support of that matter, Greylock received Plaintiff's PII. *Id.*

44. Plaintiff's PII was compromised in the Breach and stolen by cybercriminals who illegally accessed Greylock's network for the specific purposes of targeting the PII.

45. As a result of Greylock's negligence and untimely notice of the Breach, Plaintiff has already experienced damages.

46. Indeed, Plaintiff has fallen victim to at least 15 "payday loans" being applied for in his name. Plaintiff did not apply for any of these loans.

47. Notably, Plaintiff experienced these financial attacks between August 2023 and October 2023, *after* the Breach occurred and at a minimum seven (7) months *prior* to Greylock sending providing notice of the Breach to Plaintiff and Class Members.

48. Further, Plaintiff regularly receives emails from his bank notifying him that unknown actors are attempting to log into his bank account. Plaintiff has experienced similar attacks as recently as June 23, 2024.

49. The lackluster protections offered by Greylock have not limited Plaintiff's exposure to dark web criminals attempting to access his financial accounts.

50. In addition to the concrete damages mentioned above, Plaintiff continues to live in fear that his compromised PII will continue to be used by cyber criminals for nefarious purposes.

51. Plaintiff has additionally suffered lost time, interference, and inconvenience stemming from his increased vulnerability to cyber criminals arising from the dissemination of his PII.

52. As a direct and proximate result of the Breach, Plaintiff has suffered damages, and anticipates spending considerable time and money on an ongoing basis to try and mitigate the damages caused by the Breach. Plaintiff's risk of identity theft and fraud is continuous and ongoing

as a result of the Breach.

CLASS ACTION ALLEGATIONS

A. Class Action Under Fed. R. Civ. P. 23

53. This action is brought by Plaintiff as a class action pursuant to Fed. R. Civ. P. 23(b)(3), (b)(2), (b)(3) and (c)(4) and for all claims asserted herein, on behalf of himself and the following, initially defined, Nationwide Class:

> All United States residents whose personal identifiable information was accessed without authorization in the data breach announced by Greylock in April of 2024 (the "Class").

54. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

55. The proposed class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

56. **Numerosity** – Although the exact number of Class members is uncertain and can only be ascertained through appropriate discovery, including discovery of Defendant's records, the Class is so numerous that the joinder of all members is impracticable as approximately 341,000 persons were affected by the Breach. The Class is comprised of an easily ascertainable set of persons during the Class Period from Greylock's own records.

57. **Commonality & Predominance** – There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. Questions of law and fact are common to all Class members because, *inter alia*, this action concerns Defendant's common business policies, as described herein, these common questions of law and fact include, without limitation:

a. Whether Greylock engaged in the conduct as alleged herein;

b. Whether Greylock had a duty to protect PII;

c. Whether Greylock used reasonable or industry standard measures to protect Class Member's PII, particularly in light of the measures recommended by data security experts;

d. Whether Greylock adequately or properly segregated its network so as to protect employee PII;

e. Whether Greylock knew or should have known prior to the Breach that its network was susceptible to a potential data breach;

f. Whether Greylock's failure to implement data security measures allowed the breach to occur;

g. Whether Greylock was negligent in failing to implement reasonable and adequate security procedures and practices;

h. Whether Greylock should have notified the Class that it failed to use reasonable and best practices, safeguards, and data security measures to protect clients' PII;

i. Whether Greylock should have notified class members that their PII would be at risk of unauthorized disclosure;

j. Whether Greylock intentionally failed to disclose material information regarding its security measures, the risk of data interception, and the Breach;

k. Whether Greylock's acts, omissions, and nondisclosures were intended to deceive Class Members;

l. Whether Greylock's conduct violated the laws alleged;

m. Whether Greylock's conduct, including its failure to act, resulted in or was the

proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and the Class Members;

n. Whether Plaintiff and the Class Members are entitled to restitution, disgorgement, and other equitable relief; and

o. Whether Plaintiff and the Class Members are entitled to recover actual damages, statutory damages, and punitive damages.

58. **Typicality** – Plaintiff's claims are typical of the claims of the Class Members in that Plaintiff, like all Class Members, were caused harm by Greylock's failure to adequately protect its clients' PII.

59. **Adequacy of Representation** – Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who are experienced in consumer class-action litigation. Plaintiff has no interests which are adverse to, or in conflict with, other members of the Class.

60. **Superiority of Class Action** – A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. The prosecution of separate actions by the individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, a class action presents far fewer management difficulties, conserves judicial as well as the parties' resources and protects the rights of each Class member. The damages suffered by Plaintiffs and the Class members are relatively small compared to the burden and

expense required to individually litigate their claims against Greylock, and thus, individual litigation to redress Greylock's wrongful conduct would be impracticable.

B. Injunctive and Declaratory Relief

61. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

62. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Greylock failed to timely notify the public of the Breach;

b. Whether Greylock owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Greylock's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

d. Whether Greylock failed to adequately comply with industry standards amounting to negligence;

e. Whether Greylock failed to take commercially reasonable steps to safeguard the PII of Plaintiff and the class members; and,

f. Whether adherence to data security recommendations and measures recommended by data security experts would have reasonably prevented the Breach.

63. Finally, all members of the proposed class are readily ascertainable. Greylock has

access to information regarding the Breach, the time period of the Breach, and which individuals were potentially affected. Using this information, the members of the class can be identified and their contact information ascertained for purposes of providing notice to the class members.

COUNT I

NEGLIGENCE
(On Behalf of Plaintiff and the Class)

64. All previous paragraphs are incorporated as though fully set forth herein.

65. Upon accepting and storing the PII of Plaintiffs and the Class members in its computer systems and on its networks, Greylock undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Greylock knew that the PII was private and confidential and should be protected as private and confidential.

66. Greylock owed a duty of care to not subject Plaintiff, along with his PII, and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

67. Greylock owed numerous duties to Plaintiff and to the Class Members including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warning about data breaches.

68. Greylock also breached its duty to Plaintiff and the Class Members to adequately

protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Greylock failed to provide adequate supervision and oversight of the PII which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.

69. Greylock, knew or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Greylock knew about well-publicized data breaches, yet still failed to protect its clients' PII.

70. Greylock knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

71. Greylock breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiff and Class Members.

72. Because Greylock knew that a breach of its systems would damage hundreds of thousands of individuals, including Plaintiff and Class Members, Greylock had a duty to protect its data systems and the PII contained thereon.

73. Greylock had a special relationship with Plaintiff and Class Members, Plaintiff's and Class Members' willingness to entrust Greylock with their PII was predicated on the understanding that Greylock would take adequate security precautions. Further, only Greylock had the ability to protect its systems and the PII it stored on them from attack.

74. Greylock's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII. Greylock's misconduct included failing to: (1) secure its systems,

despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

75. Greylock also had independent duties under state and federal laws that required Greylock to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the data breach.

76. Greylock breached its duties to Plaintiff and the Class Members in numerous ways including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiff and the Class Members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class Members' PII both before and after learning of the Breach;

d. by failing to comply with the minimum industry standards during the period of the Breach; and

e. by failing to timely and accurately disclose that Plaintiff's and the Class Members' PII had been improperly acquired or accessed.

77. Through Greylock's acts and omissions described in this Complaint, including Greylock's failure to provide adequate security and its failure to protect PII of Plaintiff and Class Members from being foreseeably captured, accessed, disseminated, stolen and misused, Greylock unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiff

and Class Members during the time it was within Greylock's possession or control.

78. The law further imposes an affirmative duty on Greylock to timely disclose the unauthorized access and theft of the PII to Plaintiff and the Class so that Plaintiff and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

79. Greylock breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiff and Class Members and then by failing to provide Plaintiff and Class Members information regarding the Breach until April of 2024, eleven (11) months after the Breach occurred.

80. Through Greylock's acts and omissions described in this Complaint, including Greylock's failure to provide adequate security and its failure to protect PII of Plaintiff and Class Members from being foreseeably captured, accessed, disseminated, stolen, and misused, Greylock unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiff and Class Members during the time it was within Greylock's possession or control.

81. Further, through its failure to provide timely and clear notification of the Breach to its clients, Greylock prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

82. Upon information and belief, Greylock improperly and inadequately safeguarded PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Greylock's failure to take proper security measures to protect sensitive PII of Plaintiff and Class Members, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiff and the Class Members.

83. Greylock's conduct was grossly negligent and departed from all reasonable standards of care. Including but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to the PII of Plaintiff and Class Members; and failing to provide Plaintiff and Class Members with timely and sufficient notice that their sensitive PII had been compromised.

84. Neither plaintiff nor other Class Members contributed to the Breach and subsequent misuse of their PII as described in this Complaint.

85. As a direct and proximate cause of Greylock's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages arising from fraudulent loans applied for using Plaintiff's and Class Members' PII; damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of PII of Plaintiff and Class Members; damages arising from Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Breach and/or false or fraudulent charges stemming from the Breach, including, but not limited to, late fees charges and foregone cash back rewards; and/or damages from lost time and effort to mitigate the actual and potential impact of the Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of the other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II

NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

86. All previous paragraphs are incorporated as though fully set forth herein.

87. Section 5 of the FTC Act prohibits "unfair . . . practice in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Greylock, or failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1). The FTC publications and orders described above also form part of the basis for Greylock's duty in this regard.

88. Greylock violated section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Greylock's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Greylock, including, specifically, the immense damages that would result to Plaintiff and Class Members.

89. Greylock's violation of Section 5 of the FTC Act constitutes negligence per se.

90. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

91. The harm that occurred as a result of the Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

92. Greylock also violated HIPAA through its failure to protect Plaintiff's and Class Members' data to which it was entrusted.

93. Greylock's violation of HIPAA likewise constitutes negligence per se.

94. Plaintiff and Class Members are within the class of persons that HIPAA was intended to protect.

95. The harm that occurred as a result of the Breach is the type of harm HIPAA was intended to guard against.

96. As a direct and proximate result of Greylock's negligence per se, Plaintiffs and the Class Members have suffered , and continue to suffer, injuries and damages including, but not limited to: damages arising from fraudulent loans applied for using Plaintiff's and Class Members' PII ; damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of PII of Plaintiff and Class Members; damages arising from Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Breach and/or false or fraudulent charges stemming from the Breach, including, but not limited to, late fees charges and foregone cash back rewards; and/or damages from lost time and effort to mitigate the actual and potential impact of the Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

97. Greylock's breach of its duties provided the means for third parties to access, obtain, and misuse the PII of Plaintiff and the Class Members without authorization. It was reasonably foreseeable that such breaches would expose the PII to criminals and other unauthorized access.

98. Greylock's breach of its duties has directly and proximately injured Plaintiff and Class Members, including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to which their breach puts their credit, reputation, and finances at risk, and taking reasonable steps (now or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

99. Plaintiffs and the Class Members are entitled to damages in an amount to be proven at trial.

COUNT III

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class)

100. All previous paragraphs are incorporated as though fully set forth herein.

101. Greylock entered into contracts with various clients, including the DOJ, to provide litigation support. *See* Exhibit A.

102. The contracts were virtually identical to each other and were made expressly for the benefit of Plaintiff and Class Members, as it was their PII that Greylock agreed to collect and safeguard.

103. The benefit of collection and protection of the PII belonging to Plaintiff and Class Members were the direct and primary objective of the contracting parties. Thus, Plaintiff and Class Members are third-party beneficiaries to the contracts.

104. Greylock breached its contracts with its clients, including the DOJ, when it among other things, failed: (1) to provide various services to its clients for the benefit of Plaintiff and Class Members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII; and (3) to protect Plaintiff's and Class Members' PII in

compliance with federal and state laws and regulations and industry standards.

105. Protection of PII is a material term of the contracts between Plaintiff and Class Members as third-party beneficiaries, on the one hand, and Greylock, on the other hand. Had Plaintiff known that Greylock would not adequately protect its clients' PII, they would not have given their PII to Greylock.

106. Greylock did not satisfy its promises and obligations to Plaintiff and the Class Members as third-party beneficiaries under the contracts because it did not take reasonable measures to keep their PII secure and confidential, and did not comply with applicable laws, regulations, and industry standards.

107. Greylock materially breached these contracts by failing to implement adequate security measures.

108. Greylock's failure to satisfy its obligations led directly to the successful intrusion of Greylock's computer servers and stored data and led directly to unauthorized parties' access to and exfiltration of Plaintiff's and Class Members' PII.

109. As a result of Greylock's failure to implement necessary security measures, Plaintiff and Class Members have suffered actual damages resulting both from the theft of their PII and remain at imminent risk of suffering additional damages in the future.

110. Accordingly, Plaintiff and Class Members as third-party beneficiaries have been injured as a proximate result of Greylock's breaches of contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV

UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

111. All previous paragraphs are incorporated as though fully set forth herein.

112. Plaintiff brings this Count in the alternative to the breach of third-party beneficiary contract count above.

113. Plaintiff and Class Members conferred a monetary benefit on Greylock by way of providing Greylock with their PII through Defendant's clients. In exchange, Plaintiff and Class Members should have had their private information protected with adequate data security.

114. Greylock knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it.

115. Greylock profited from Plaintiff's and Class Members' retained PII and used Plaintiff's and Cass Members' PII for business purposes.

116. Greylock failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

117. Greylock acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

118. Had Plaintiff and Class Members known that Greylock would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have entrusted their PII to Greylock.

119. Plaintiff and Class Members have no adequate remedy at law.

120. Under the circumstances, it would be unjust for Greylock to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

121. As a direct and proximate result of Greylock's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii); lost or diminished value of their PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Breach; (v) actual misuse of

the compromised PII consisting of an increase in spam calls, texts, and/or email; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and increased risk to their PII, which: (a) remains unencrypted and available for unauthorized possession and is subject to further unauthorized disclosures so long as Greylock fails to undertake appropriate and adequate measures to protect the Private Information.

122. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Greylock and/or an order proportionally disgorging all profits, benefits and other compensation obtained by Greylock from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

123. Plaintiff and Class Members may not have an adequate remedy at law against Greylock, and accordingly they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V

DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

124. All previous paragraphs are incorporated as though fully set forth herein.

125. As previously alleged, Plaintiff and Class Members were third-party beneficiaries to contracts that required Greylock to provide adequate security for the PII it collected from its clients. As previously alleged, Greylock owes duties of care to Plaintiff and Class Members that require it to adequately secure PII.

126. Greylock still possesses PII pertaining to Plaintiffs and Class Members.

127. Greylock has made no announcement that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

128. Accordingly, Greylock has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Greylock's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

129. Actual harm has arisen in the wake of the Greylock Breach regarding Greylock's contractual obligations and duties of care to provide data security measures to Plaintiff and Class Members.

130. Plaintiff therefore seeks a declaration that (a) Greylock's existing data security measures to not comply with its contractual obligations and duties of care, and (b) in order to comply with ins contractual duties of care, Greylock must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Greylock's systems on a periodic basis, and ordering Greylock to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting PII by, among other things, creating firewalls and access controls so that if one are of Greylock is compromised, hackers cannot gain access to other portions of Greylock's systems;

e. Purging, deleting, and destroying in a reasonable secure manner PII not

necessary for its provisions of services;

f. Conducting regular database scanning and securing checks;

g. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Educating its clients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Greylock clients must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and/or on behalf of himself and all other similarly situated members of the Class members, respectfully requests the Court grant the following relief:

A. Certification of the action as a class action under Rule 23 on behalf of the Class;

B. Designation of Plaintiff as representative of the Class;

C. Designation of Plaintiff's counsel as class counsel;

D. For equitable and injunctive relief enjoining Greylock from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs' and the Class Members' PII;

E. An Order compelling Greylock to employ and maintain appropriate systems and policies to protect consumer PII and to promptly detect, and timely and accurately report, any unauthorized access to that data;

F. For equitable, declaratory, and injunctive relief;

G. For compensatory damages sustained by Plaintiffs and Class members;

H. For payment of costs of suit herein incurred;

I. For both pre-judgment and post-judgment interest on any amounts awarded;

J. For punitive damages;

K. For payment of reasonable attorneys' fees, expert fees, and expenses, as may be allowable under applicable law; and

L. For such other and further relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff Michael Rosen, on behalf of himself and all others similarly situated, hereby demands a jury trial with respect to all issues triable of right by jury.

Dated: July 22, 2024

Respectfully submitted,

/s/ Vishal H. Shah

Vishal H. Shah (BBO No. 708838)
SHAH LITIGATION, PLLC
867 Boylston St., 5th Fl. #1893
Boston, Massachusetts 02116
t: (617) 334-5825
vishal@shahlitigation.com

Charles J. Kocher*
Tyler J. Burrell (BBO No. 712158)
Gaetano J. DiPersia*
McOMBER McOMBER & LUBER, P.C.
50 Lake Center Drive, Suite 400
Marlton, New Jersey 08053
t: (856) 985-9800
cjk@njlegal.com
tjb@njlegal.com
gjd@njlegal.com

Attorneys for Class Representative Plaintiff Michael Rosen, on behalf of himself and all others similarly situated for the Rule 23(b)(3) Class

* motion for *pro hac vice* admission forthcoming